# SPYWOLF

## Security Audit Report

Completed on

**May 24, 2023**

# OVERVIEW

This audit has been prepared for **PEPE Yield** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

*The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal*

- SPYWOLF Team -

# TABLE OF CONTENTS

# PEPE Yield

## PROJECT DESCRIPTION

**According to their whitepaper:**

Pepe Yield provides a decentralized financial asset which rewards users with a sustainable fixed compound interest model through use of it's unique SAP protocol.

The Pepe Yield Auto-Staking Protocol (PAP for short) is a financial protocol that makes staking easier, more efficient and awards $PEPY token holders the highest stable returns in crypto.

**Release Date:** Presale starts in May, 2023

**Category:** Staking

# CONTRACT INFO

Token Name
Pepe Yield

Symbol
PEPY

Contract Address
0x7cBFa78a082Bb4810D3601d761b8e260c13F6AD9

Network
Binance Smart Chain

Language
Solidity

Deployment Date
May 24, 2023

Verified?
Yes

Total Supply
325,000

Status
Not launched

# TAXES

Buy Tax
**4%**

Sell Tax
**5%**

*Taxes can be changed in future

# Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

**Blockchain security tools used:**

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

# TOKEN TRANSFERS STATS

| | |
|---|---|
| **Transfer Count** | 3 |
| **Uniq Senders** | 2 |
| **Uniq Receivers** | 3 |
| **Total Amount** | 650000 PEPY |
| **Median Transfer Amount** | 296900 PEPY |
| **Average Transfer Amount** | 216666.6666666667 PEPY |
| **First transfer date** | 2023-05-24 |
| **Last transfer date** | 2023-05-24 |
| **Days token transferred** | 1 |

# SMART CONTRACT STATS

| | |
|---|---|
| **Calls Count** | 9 |
| **External calls** | 5 |
| **Internal calls** | 4 |
| **Transactions count** | 6 |
| **Uniq Callers** | 3 |
| **Days contract called** | 1 |
| **Last transaction time** | 2023-05-24 01:52:32 UTC |
| **Created** | 2023-05-24 01:32:35 UTC |
| **Create TX** | 0xab0b4604db540413aca0bacbbdbddc96908f316b93549cbd6b994ff2671621e5 |
| **Creator** | 0x06be72545953bfcba236146a88740e1d7a3f8155 |

# VULNERABILITY CHECK

| | |
|---|---|
| Design Logic | Passed |
| Compiler warnings. | Passed |
| Private user data leaks | Passed |
| Timestamp dependence | Passed |
| Integer overflow and underflow | Passed |
| Race conditions and reentrancy. Cross-function race conditions | Passed |
| Possible delays in data delivery | Passed |
| Oracle calls | Passed |
| Front running | Passed |
| DoS with Revert | Passed |
| DoS with block gas limit | Passed |
| Methods execution permissions | Passed |
| Economy model | Passed |
| Impact of the exchange rate on the logic | Passed |
| Malicious Event log | Passed |
| Scoping and declarations | Passed |
| Uninitialized storage pointers | Passed |
| Arithmetic accuracy | Passed |
| Cross-function race conditions | Passed |
| Safe Zeppelin module | Passed |
| Fallback function security | Passed |

# THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

## High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

## Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

## Low Risk

Issues on this level are minor details and warning that can remain unfixed.

## Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

# FOUND THREATS

## ⚠ High Risk

Owner can blacklist address, making it impossible to sell.
If liquidity pair is blacklisted, it will become impossible to sell for all users.

```
function setBotBlacklist(address _botAddress, bool _flag) external onlyOwner {
    require(isContract(_botAddress), "only contract address, not allowed exteranlly owned account");
    blacklist[_botAddress] = _flag;
}

function _transferFrom(
    address sender,
    address recipient,
    uint256 amount
) internal returns (bool) {

    require(!blacklist[sender] && !blacklist[recipient], "in_blacklist");
.....................
}
```

- Recommendation:
  - Considered as good bot protection practice is blacklisting addresses to be automated for short period after initial liquidity add.

# Informational

This is rebase token with increasing supply up to 3,250,000,000. Increasing supply over time may lead to token's price inflation.

```
uint256 private constant MAX_SUPPLY = 325 * 10**7 * 10**DECIMALS;
uint256 private constant INITIAL_FRAGMENTS_SUPPLY = 325 * 10**3 * 10**DECIMALS;
```

```
function _transferFrom(address sender, address recipient, uint256 amount) internal returns (bool) {
.....................
if (shouldRebase()) {
   rebase();
}
.....................
}

function shouldRebase() internal view returns (bool) {
    return
        _autoRebase &&
        (_totalSupply < MAX_SUPPLY) &&
        msg.sender != pair  &&
        !inSwap &&
        block.timestamp >= (_lastRebasedTime + 15 minutes);
}

function rebase() internal {

    if ( inSwap ) return;
    uint256 rebaseRate;
    uint256 deltaTimeFromInit = block.timestamp - _initRebaseStartTime;
    uint256 deltaTime = block.timestamp - _lastRebasedTime;
    uint256 times = deltaTime.div(15 minutes);
    uint256 epoch = times.mul(15);

    if (deltaTimeFromInit < (365 days)) {
        rebaseRate = 2355;
    } else if (deltaTimeFromInit >= (365 days)) {
        rebaseRate = 211;
    } else if (deltaTimeFromInit >= ((15 * 365 days) / 10)) {
        rebaseRate = 14;
    } else if (deltaTimeFromInit >= (7 * 365 days)) {
        rebaseRate = 2;
    }

    for (uint256 i = 0; i < times; i++) {
        _totalSupply = _totalSupply
            .mul((10**RATE_DECIMALS).add(rebaseRate))
            .div(10**RATE_DECIMALS);
    }

    _gonsPerFragment = TOTAL_GONS.div(_totalSupply);
    _lastRebasedTime = _lastRebasedTime.add(times.mul(15 minutes));

    pairContract.sync();

    emit LogRebase(epoch, _totalSupply);
}
```

# Informational

Owner can manual swap accumulated tokens in the contract.

```
function withdrawAllToTreasury() external swapping onlyOwner {

    uint256 amountToSwap = _gonBalances[address(this)].div(_gonsPerFragment);
    require( amountToSwap > 0,"There is no PEPY token deposited in token contract");
    address[] memory path = new address[](2);
    path[0] = address(this);
    path[1] = router.WETH();
    router.swapExactTokensForETHSupportingFeeOnTransferTokens(
        amountToSwap,
        0,
        path,
        treasuryReceiver,
        block.timestamp
    );
}
```

Owner can change fees address receivers.

```
function setFeeReceivers(
    address _autoLiquidityReceiver,
    address _treasuryReceiver,
    address _yieldInsuranceFundReceiver,
    address _firePit
) external onlyOwner {
    autoLiquidityReceiver = _autoLiquidityReceiver;
    treasuryReceiver = _treasuryReceiver;
    yieldInsuranceFundReceiver = _yieldInsuranceFundReceiver;
    firePit = _firePit;
}
```

# Informational

Owner can exclude address from fees.
When address is excluded from fees, the user will receive the whole amount of the bought, sold and/or transferred tokens.

```
function setWhitelist(address _addr) external onlyOwner {
    _isFeeExempt[_addr] = true;
}
```

Owner can turn rebase on/off.

```
function setAutoRebase(bool _flag) external onlyOwner {
    if (_flag) {
        _autoRebase = _flag;
        _lastRebasedTime = block.timestamp;
    } else {
        _autoRebase = _flag;
    }
}
```

RECOMMENDATIONS FOR

# GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

## PEPE Yield

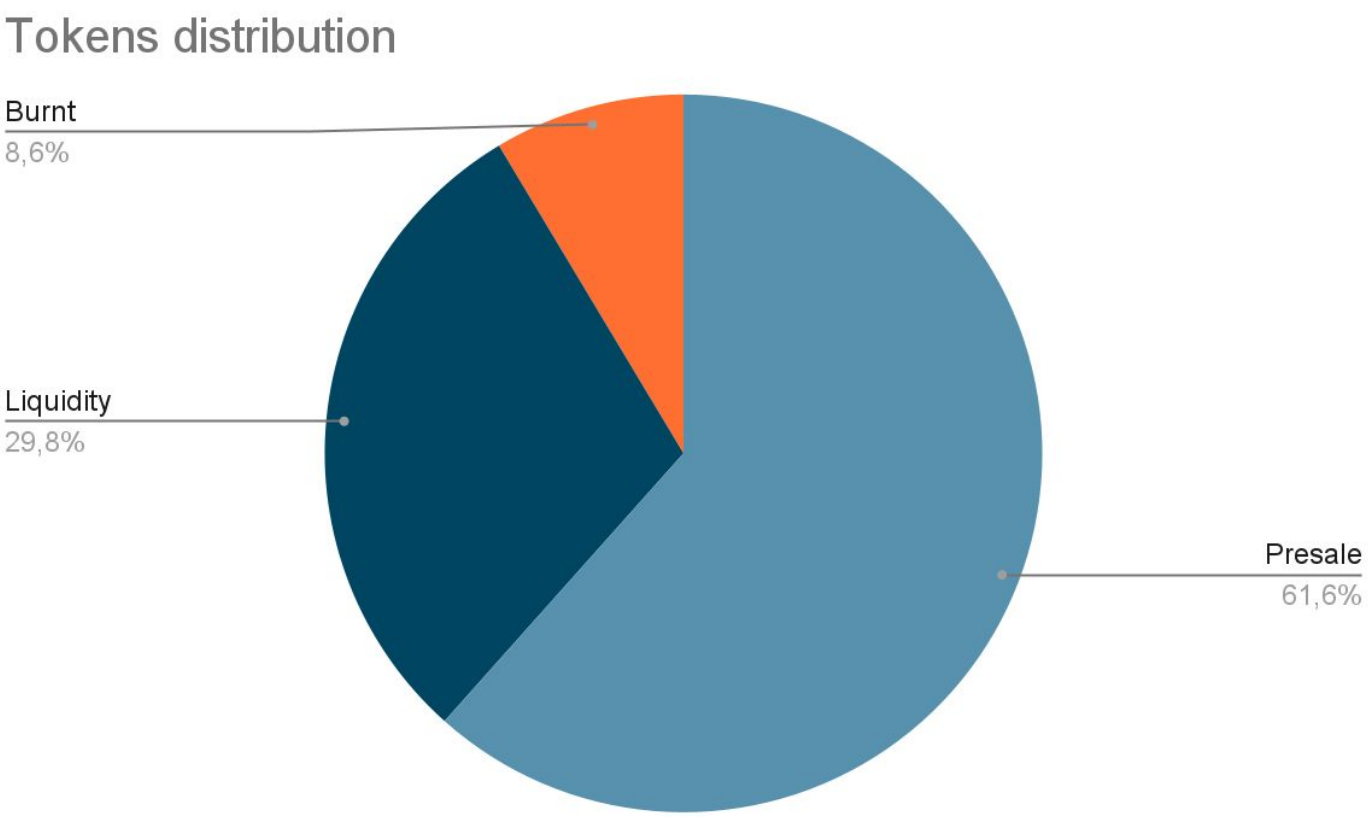
### GOOD PRACTICES FOUND

- ✔ The owner cannot set a transaction limit
- ✔ The smart contract utilizes "SafeMath" to prevent overflows

# TOKENOMICS

The following tokenomics are based on the Pinksale's presalge page:

- 61.6% - Presale
- 29.8% - Liquidity
- 8.6% - Burnt



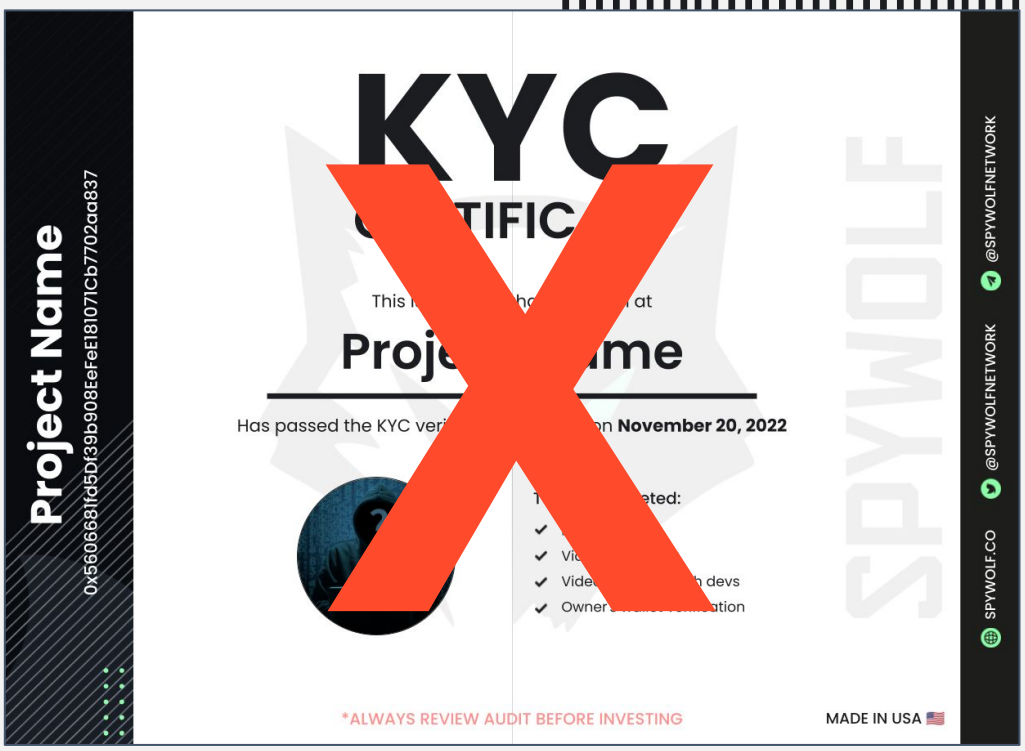
# THE TEAM

⚠️ The team is annonymous

## KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



# WEBSITE

## Website URL
https://pepeyield.com/

## Domain Registry
https://www.registrar.eu

## Domain Expiration
2024-05-23

## Technical SEO Test
Passed

## Security Test
Passed. SSL certificate present

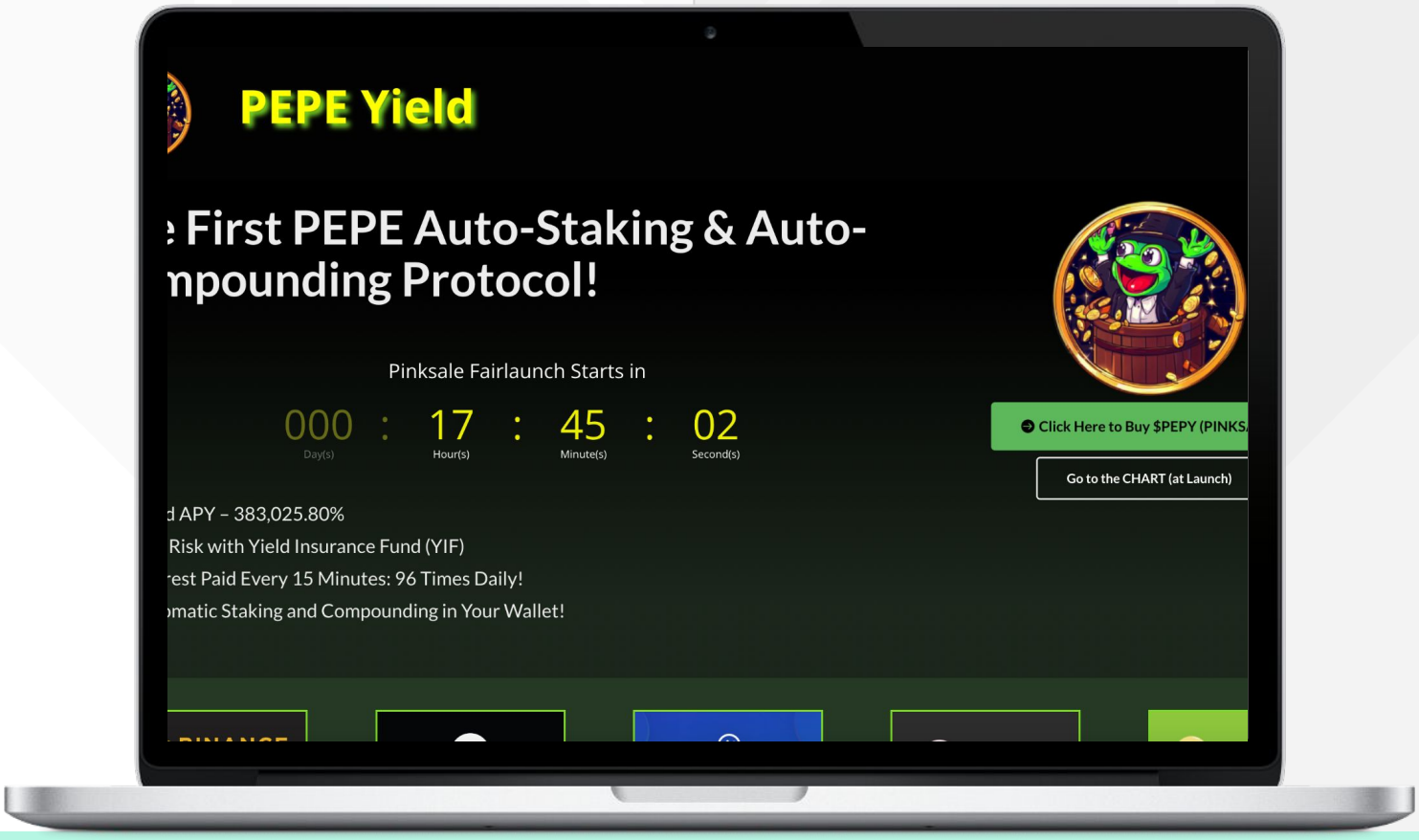
## Design
Single page design with appropriate color scheme and graphics.

## Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

## Whitepaper
Well written, explanatory.

## Roadmap
Yes, goals set without time frames.

## Mobile-friendly?
Yes



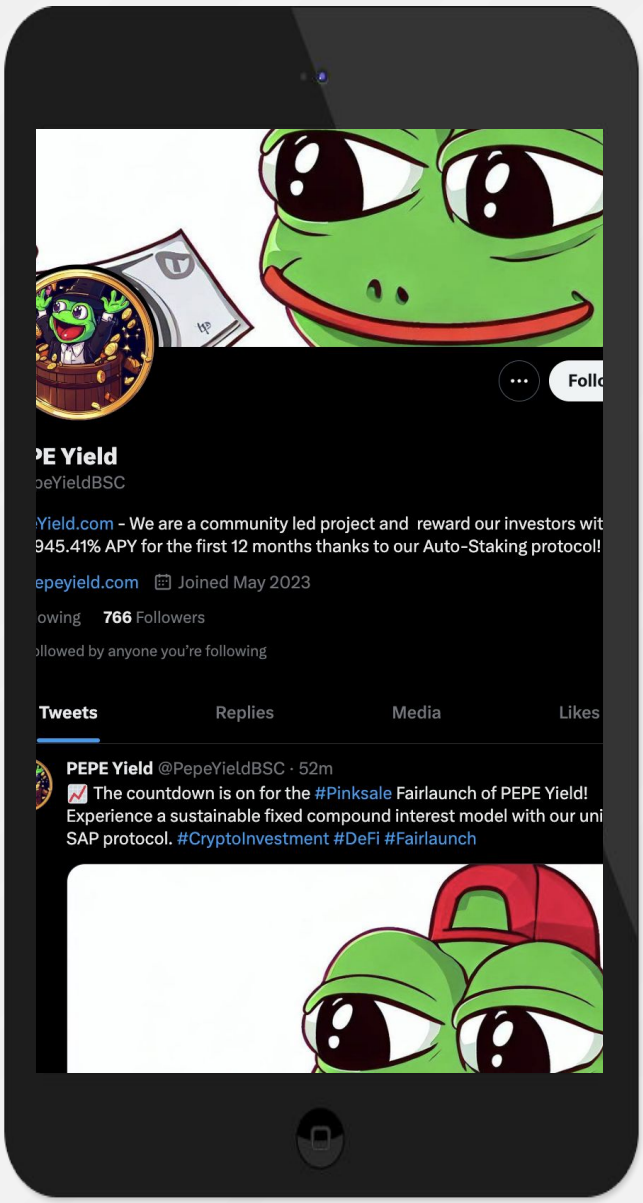

# pepeyield.com

# SOCIAL MEDIA

## & ONLINE PRESENCE

**ANALYSIS**

**Project's social media pages are active**




**Twitter**

@pepeyieldbsc

- 290 followers
- 2 total posts
- New account

**Discord**

- Not available

**Telegram**

@pepeyield

- 159 members
- Active users
- Active mods

**Medium**

- Not available

# SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

# ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 500 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

## FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

# Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

**DISCLAIMER:**
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.